IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TENNESSEE

STATE OF TENNESSEE

COUNTY OF SHELBY

Case No. 23-SW-515

ATTACHMENT C

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, **Keyotta Sanford**, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the FBI assigned to the Memphis Division and have been a Special Agent since January 2019. I am currently assigned to the Child Exploitation & Human Trafficking Task Force, investigating matters involving the sexual exploitation of children, human trafficking, and child sexual abuse material (CSAM). I have participated in various trainings and investigations involving online and computer related offenses and have executed numerous search warrants, including those involving searches and seizure of computers, digital media and electronically stored information.

2. I make this affidavit in support of an application for a search warrant for information associated with a certain Google accounts associated with the identifier, **"jarrodsanford81@gmail.com"** and **"jarrod81sanford@gmail.com"** that is stored at premises controlled by Google LLC ("Google"), which is an electronic communications and remote computing service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in **Attachment A**. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2251(a) (production of child pornography) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)

KS
12/20/23

(possession of and access with intent to view child pornography) to require Google to disclose to the government copies of the information (including the content of communications) further described in **Section I of Attachment B**. Upon receipt of the information described in **Section I of Attachment B**, government-authorized persons will review that information to locate the items described in **Section II of Attachment B**.

3. The statements in this affidavit are based in part on information provided by other sworn law enforcement officers participating in this investigation, through observations and conversations of your affiant personally, and through other sources specifically named in this affidavit. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence in violation of 18 U.S.C. § 2251(a) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) will be located at the premises described in **Attachment A**, and that evidence will be in the form of the items listed in **Attachment B**, both of which are incorporated by reference as if fully set forth herein.

STATUTORY AUTHORITY

4. 18 U.S.C. §§ 2251(a) makes it a federal offense for anyone to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in sexually explicit conduct as defined in 18 U.S.C. §§ 2256, for the purpose of producing a visual depiction of such conduct, or attempts to do so.

5. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has

KS
12/20/23

been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this affidavit and **Attachment B**:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

KS
12/20/23

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

f. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the internet service provider (ISP) assigns a different unique number to a computer every time it accesses the

IC
12/20/23

Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

h. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

i. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

j. "Records," "documents," and "materials," as used herein, include all information recorded in any form and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

k. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

l. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

KS
12/20/23

CHARACTERISTICS OF INDIVIDUALS WHO PRODUCE AND POSSESS CHILD PORNOGRAPHY

7. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, there are certain characteristics that are prevalent among individuals who are involved in the production and receipt of child pornography:

a. The majority of individuals who produce and possess child pornography are persons who have a sexual attraction to children, and may engage in the sexual abuse of children or exchange and collect child pornography and child erotica to receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.

b. Individuals who produce and possess child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videos, drawings or other visual media. Not only do these individuals oftentimes use these materials for their own sexual arousal and gratification, but they also may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. The majority of individuals who collect, receive and produce child pornography often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. Individuals who collect and produce child pornography often correspond with and/or meet others to share information and materials and often maintain lists of names, usernames, addresses, emails, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography and child sexual abuse.

KS
12/20/23

d. Persons committing these criminal acts, more likely than not, almost always possess and maintain their hard copy and/or digital medium collections of child pornographic and child erotica material in a secure and private environment. Due to the psychological support their collections provide, such individuals find comfort and justification for their illicit behavior and desires and rarely destroy such materials. As such, these collections are often maintained for several years and are kept close by, usually in a location that is mobile and/or easily accessible to the individual.

e. In some cases, people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers of digital devices. Traces of such activity can often be found on computers or digital devices for months or even years after any downloaded files have been deleted.

f. Individuals that produce and possess child pornography frequently prefer not to be without their child pornography for any prolonged time period, and more likely than not may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage. This behavior has been documented by law enforcement officers involved in child exploitation and pornography investigations worldwide.

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

8. On November 20, 2023, the FBI Memphis Child Exploitation and Human Trafficking Task Force (CEHTTF) received a tip from the Tipton County Sheriff's Office (TCSO) regarding allegations that a registered sex offender had taken nude images of a13-year-old relative.

9. According to the TCSO, on or around 11/19/2023, Deputies responded to complaint in Covington, TN involving the sexual assault of a 13-year-old female by a relative. Deputies identified the victim's relative as Jarrod Sanford (Sanford), who was a registered sex offender. While on scene, the minor victim told the Deputies that Sanford had sexually assaulted her the day

KS
12/20/23

prior. The victim also provided Deputies with a cell phone that she advised belonged to Sanford, who had given it to her when police arrived at the residence. Sanford told her that he did not want the phone to be provided to law enforcement. Additionally, the minor told Deputies that she believed Sanford had taken nude images of her utilizing the phone.

10. On November 20, 2023, a child forensic interview was conducted with the minor victim. During her interview, the victim disclosed she had been sexually assaulted by Sanford on more than one occasion. The minor confirmed she told police that Sanford had taken nude images of her and recalled an incident in which she could hear a noise similar to that of a cell phone taking a picture and recording a video. The minor further advised that this occurred while she was being sexually assaulted by Sanford and while he was holding her head down.

11. On November 20, 2023, a State of Tennessee search warrant was issued for a black and silver in color Android cell phone, which was provided to TCSO Deputies and identified as being used by Sanford to take nude images of the minor victim.

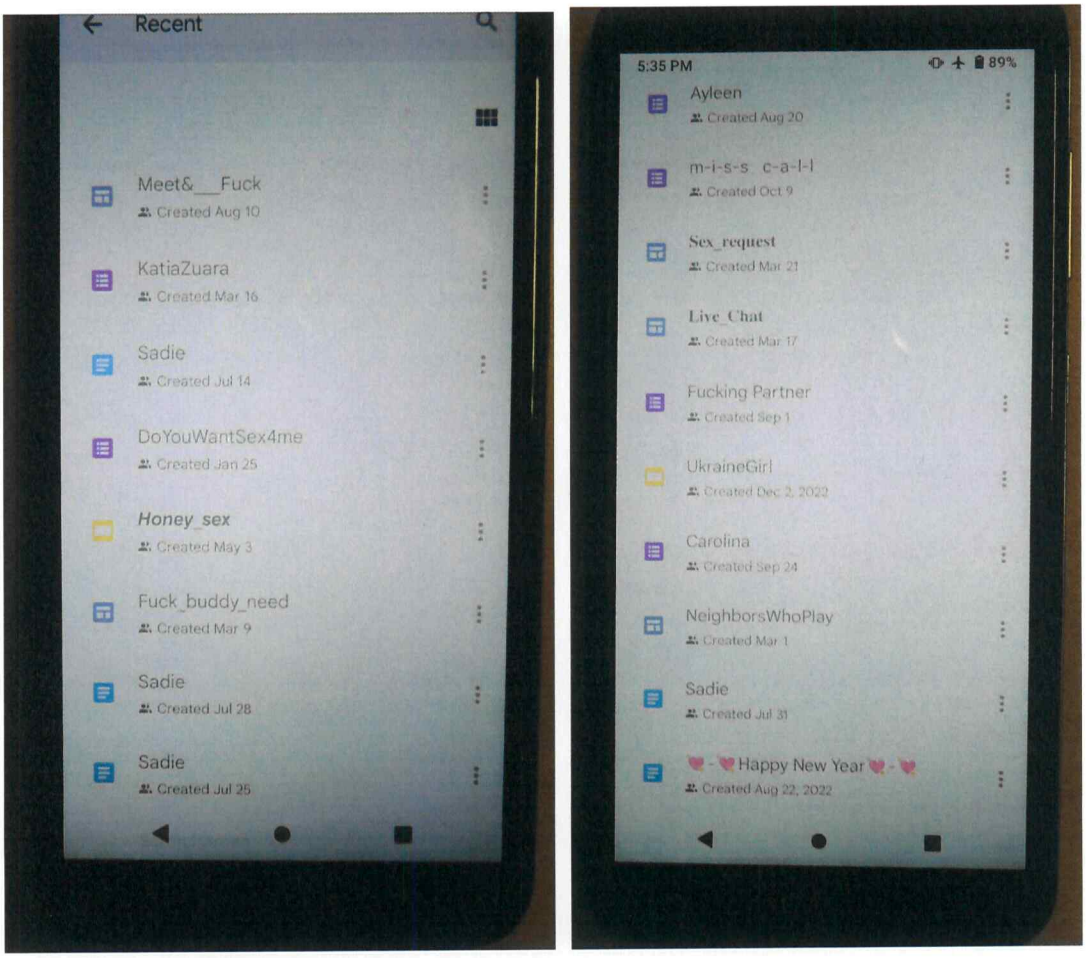
12. On November 20, 2023, your affiant confirmed with the U.S. Attorney's Office and the U.S. Probation Office that Jarrod Steven Sanford was on Federal Probation for life due to sexual offenses and was not allowed to have any media devices that were not monitored by the U.S. Probation Office.

13. On November 21, 2023, a federal search warrant was executed on the Android cell phone, which was identified as being utilized by Sanford to take nude images of the minor victim. Pursuant a forensic examination of the device, images consistent with CSAM were observed. In particular, your affiant observed what appeared to be images an unknown female performing oral sex on an unknown male. Based on a comparison of a known image of the minor victim, it was believed the unknown female and the minor victim were one and the same. Your affiant also

KS
12/20/23

observed an image of what appeared to be an individual holding a cell phone, with a picture of nude erect penis visible on the screen.

14. An analysis of the device also showed the phone was registered to Google utilizing the email account jarrodsanford81@gmail.com. Associated with the Google account was a Google Drive, which your affiant knows is Google's cloud based storage service and can be used to store and access documents, photos, and other files across all of a user's Internet accessible devices. Your affiant observed what appeared to be files within the "Recent" section of the Google Drive, with many of the files having names containing sexual references or being associated with female names. Below are pictures of some of the file names observed on the device and associated with the Google Drive:



KS
12/20/23

15. On November 22, 2023, investigators interviewed an adult relative of the minor victim. During the interview, the minor victim was positively identified as the unknown female performing oral sex on an unknown male.

16. On November 22, 2023, a federal arrest warrant was issued for Sanford, who was later detained that same day by the U.S. Marshals. He was arrested in his truck, and in the center console of the truck the deputy marshals found a black in color Android cell phone, with the word "BLU" displayed on the back. They seized the phone and identified it as belonging to Sanford. Pursuant forensic examination of the device, an analysis of the device showed the BLU Android phone was registered to the same Google account, associated with the email address jarrodsanford81@gmail.com, as the black and silver colored Android cell phone which contained CSAM of the minor victim. Unlike with the previous phone, your affiant did not observe files within the "Recent" section of the Google Drive.

17. On November 27, 2023, the minor victim was forensically interviewed by a FBI Child Adolescent Forensic Interviewer. During the interview, the minor victim was shown images which were obtained from a forensic extraction of an Android cell phone, identified as belonging to Sanford. The minor victim positively identified herself within the images and advised Sanford had forced her to perform oral sex on him, in the living room of his residence. The minor victim also disclosed being sexually assaulted by Sanford on numerous occasions, starting around when she was approximately 12 years of age. The sexual assaults occurred within Sanford's residence in Covington, Tennessee.

18. On November 28, 2023, a State of Tennessee search warrant was issued to search the residence of Sanford, located at 2154 Bringle Rd, Covington, Tennessee 38019, which was identified by the minor victim as the place in which she was sexually assaulted by Sanford. TCSO

KS
12/20/23

Deputies identified and seized multiple additional electronic devices, some of which were believed to have been unauthorized and against the terms of Sanford's probation. Pursuant to a forensic extraction of a Samsung Galaxy Tab, an analysis of the device showed it was registered to Google utilizing the email account jarrod81sanford@gmail.com. Further analysis of the device showed it belonged to Sanford and was most likely considered an "authorized" device which was being monitored. As such, there was no CSAM observed; however, there were images of the minor victim during the timeframe of the alleged criminal activity, which also appeared to have been backed up to the cloud.

19. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. § 2251(a) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) have been committed, and evidence, instrumentalities and fruits of those violations are located on the Google accounts further described in **Attachments A and B** of this affidavit.

INFORMATION REGARDING GOOGLE

20. Based on my knowledge and experience, I know that Google LLC ("Google") is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2), headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. Google provides a variety of on-line services, including cloud file storage, to the public. Google allows subscribers to obtain email accounts at the domain name "gmail.com," like the account listed in **Attachment A**. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information; therefore, the computers and servers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account

KS
12/20/23

information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

15. In addition, a Google subscriber can store on servers maintained or owned by Google other files related or in addition to the email, such as contact lists, address books, calendar data, images and videos. Through training and experience, your Affiant is aware that evidence of who was using a Google account can frequently be found in these related files.

16. In my training and experience, Internet Service Providers (ISP) generally ask their subscribers to provide certain personal identifying information when registering for an account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

17. ISP's typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, ISP often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses

KS
12/20/23

associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google account.

18. In some cases, ISP account users will communicate directly with an ISP about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. ISP providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. [1]

[1] It is possible that Google stores some portion of the information sought outside of the United States. Under the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") the Stored Communications Act was amended to require that communications providers in the United States respond to legal process and return relevant data regardless of the location of the servers containing the data.

KS
12/20/23

BACKGROUND ON CHILD EXPLOITATION MATERIAL

20. Your Affiant, through training and experience, is aware that individuals who have an interest in possessing and sharing visual depictions of minors engaging in sexually explicit conduct ("child pornography") frequently maintain collections of images they have obtained, often for time periods of several years and longer. Digital storage options are numerous, and the storage capacity has increased, allowing for the concealment and maintenance of collections of images. Furthermore, mobile devices allow for easy access to accounts, such as email, that are stored on remote servers, making it easy for collectors to conceal their interest in child exploitation from friends, co-workers, and family members while simultaneously allowing ease of access. In addition, the declining cost of digital storage devices facilitates the maintenance of ever larger collections. Your affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers. Individuals that produce and collect child pornography, more likely than not, use online resources such as companies that provide electronic communication and "cloud based" services to retrieve and store child pornography and child erotica. Electronic communication service providers, such as Gmail, Apple, Microsoft, and Dropbox among others, can be utilized for online storage which can be accessed from any Internet connected device, such as a computer or mobile phone. Even in cases when online storage is used, evidence of child pornography can be found on the user's electronic devices in most cases.

KS
12/20/23

JURISDICTION

21. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

CONCLUSION

22. I believe that based upon the totality of facts and circumstances described above, probable cause for evidence and instrumentalities of and concerning violations of 18 U.S.C. § 2251(a) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) to be located within the Google accounts jarrodsanford81@gmail.com and jarrod81sanford@gmail.com listed in **Attachment B** of this affidavit, which is incorporated by reference as if fully set forth herein, and is believed to be contained on servers and digital storage media maintained by and under the control of Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California, 94043. Your affiant requests authority to search for and seize such material.

23. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

KS
12/20/23

24. Your affiant is aware that many providers of digital services, such as email accounts, have staff members who work shifts other than traditional business hours. Such staff members may at times be responsible for compiling materials responsive to search warrants. Therefore, your affiant requests that this warrant be executable at any time of the day or night, as that may be more convenient for the responding party.

25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

26. This is an ongoing investigation. Due to the volatile nature of digital data, your affiant is aware that if notified of the existence of a search warrant, many individuals will take steps to delete other materials that may have evidentiary value pertaining to the criminal violations described herein. Therefore, your affiant requests this Court also issue an order to Google that precludes Google from notifying the subscriber of the accounts jarrodsanford81@gmail.com and jarrod81sanford@gmail.com that a search warrant has been authorized or that an investigation is underway. Your affiant is also aware that closing an account can indicate to a subscriber that the subscriber is under investigation. Therefore, your affiant further requests that this Court order Google to refrain from unilaterally closing the accounts referenced herein to preserve the integrity of the investigation and prevent destruction of potential evidence.

KS
12/20/23

27. In consideration of the foregoing, your affiant respectfully requests that this Court issue a search warrant authorizing the examination, analysis and review of the devices more specifically described in **Attachment A**, authorizing the search and seizure of the items described in **Attachment B**, incorporated herein.

AND FURTHER, AFFIANT SAITH NOT.

Keyotta Sanford - AFFIANT
Special Agent,
Federal Bureau of Investigation.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 41 by telephone, this 20th day of December, 2023.

HON. CHARMIANE G. CLAXTON
United States Magistrate Judge

KS
12/20/23